PATENT

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Inventor: Sprunk, et al.	)	Confirmation No.: 7975
	)	
	)	Customer No.: 000043471
U.S. Serial No.: 10/049,812	)	
	)	Art Unit: 2136
Filed: December 27, 2001	)	
	)	Examiner: Hoffman, Brandon S.
	)	

Title: MULTIPLE LEVEL PUBLIC KEY HEIRARCHY FOR PERFORMANCE AND HIGH SECURITY

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REMARKS FOR PRE-APPEAL BRIEF REQUEST FOR INTERVIEW

Dear Sir:

Applicants respectfully submit that the Examiner's rejections include clear errors because one or more limitations are not met by the cited reference.

I. Rejection under 35 U.S.C. § 102(b)

Claims 16-19 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Lewis (U.S. Patent No. 5,761,306, issued June 2, 1998). Applicants disagree.

Lewis discloses a public key replacement apparatus and method for operating over insecure networks. An active public key and the mask of a replacement public key are provided by a key server to nodes where the active key is used to encrypt and verify messages. To replace the active public key with the replacement public key, a key replacement message is sent to the node. The key replacement message contains the replacement public key and contains the mask of the next replacement key. The mask of the replacement public key may be generated by hashing or encrypting. The key replacement message is signed by the active public key and the replacement public key. Nodes are implemented by a computer, a smart card, a stored data card in combination with a publicly accessible node machine, or other apparatus for sending and/or receiving messages. In a particular application, a financial transaction network, nodes are consumer nodes, merchant nodes, or both, and transactions are securely sent over a possible insecure network.

Applicants submit that Lewis fails to disclose "encrypting the first key with a second key", as recited in claim 16. Specifically, Applicants' independent claim 16 reads as follows:

16. A method of updating a cryptographic key used for decrypting distributed data, the method comprising:

generating a first key for decrypting the distributed data, the first key of a first length;

encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length; and

distributing the encrypted first key. (emphasis added)

The present invention uses multiple public/private key pairs of varying levels of security. The lower-security level includes keys which are small in length, which are changed relatively often, and which require low resources to implement their coding functions. When it is desired to change key pairs of low security, a key pair at a higher security level (i.e., longer length keys) than the lower-security level keys is used to transfer the new lower-security public keys to devices using the higher-security keys. The higher security keys can, in turn, be changed at a frequency lower than the lower-security keys. The higher-security keys require a higher level of resources to perform their coding operations. This approach of using keys of escalating levels of security to replace lower-security keys, where the higher-security keys require more resources, are more secure, and are replaced less often than the lower-security keys, can be followed as many times as is desired to create a hierarchy of public key uses with the result that the lower-security operations can be performed quickly while the overall system security is high.

In contrast, Lewis discloses encrypting a replacement key but fails to disclose encrypting the replacement key with a second key. (See Lewis, col. 9, lines 26-32) In addition, since Lewis fails to disclose encrypting using a second key, Lewis necessarily also fails to disclose a second key of a second length, wherein the second length is longer than the first length. Lewis is completely devoid of the disclosure of encrypting a replacement key with a second key in the manner recited by Applicants' claims.

Therefore, Applicants submit that independent claim 16 is patentable over Lewis. Claims 17-19 are patentable at least by virtue of depending from their respective base claim. Applicants respectfully request withdrawal of the rejection.

<u>II. Rejection under 35 U.S.C. § 103(a)</u>

Claims 1-7 and 10-15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis in view of Schneier ("Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, pps. 183-184) (Schneier). Applicant respectfully disagrees.

Applicants submit that Lewis in view of Schneier fails to disclose that "the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and that requires a second cryptographic processing time greater than the first cryptographic processing time" as recited in Applicants' independent claim 1. Applicants also submit that Lewis in view of Schneier fails to disclose that "the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources" as recited in Applicants' independent claim 10.

As stated above in Section I., Lewis fails to disclose "encrypting the first key with a second key". Thus since Lewis fails to disclose a second key, Lewis also necessarily fails to disclose that "the second key…requires a second cryptographic processing time greater than the first cryptographic processing time", as recited in claim 1 or "the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources", as recited in claim 10. The Examiner conceded that Lewis fails to disclose "wherein the second key is at a second rate that is less often than the first rate". In order to cure the Examiner's perceived deficiency of Lewis, Schneier is cited.

Schneier discloses "encrypting each file with a unique file key, and then encrypting all the file keys with a key-encryption key. However, Schneier, like Lewis fails to disclose that "the second key…requires a second cryptographic processing time greater than the first cryptographic processing time", as recited in claim 1 or "the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources", as recited in claim 10.

As stated in Applicants' previous response, the cited portion of Schneier discusses the lifetime of keys and the reasons for periodically replacing keys. However, the cited portion of Schneier does not discuss methods of performing key replacements. Therefore, the cited portion of Schneier also says nothing about the length, complexity, time to process, resources to process, etc. of the replacement key relative to that of the key used to process the replacement key.

In view of the above arguments, Applicants submit that independent claims 1 and 10 are patentable over Lewis in view of Schneier. Claims 2-7 and 11-15 are patentable at least by virtue of depending from their respective base claim. Applicants respectfully request withdrawal of the rejection.

Date: July 27, 2006

Respectfully submitted,

By: /Thomas Bethea, Jr./
Thomas Bethea, Jr.
Reg. No.: 53,987

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1850

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional) D02236-03
	Application Number 10/049812,124	Filed 12/27/2001
	First Named Inventor Eric Sprunk	
	Art Unit 2136	Examiner Hoffman, Brandon S.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheets(s).
Note: No more than five (5) pages may be provided.

I am the

□ applicant inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

□ attorney or agent of record.
Registraton number ____________

☒ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34: 53,987

/Thomas Bethea, Jr./
Signature

Thomas Bethea, Jr.
Typed or printed name

215-323-1850
Telephone number

July 27, 2006
Date

NOTE: Signatures of all the inventors or assignees or record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, se below*

☒ *Total of 1 forms are submitted.